RECEIVED
CENTRAL FAX CENTER
OCT 19 2007

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 1033-T00534C

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on 10-19-07

Signature: [signature]

Typed or printed name: Jeancaux Jordan

Application Number	Filed
10/605,689	October 17, 2003

First Named Inventor: James M. Doherty, et al.

Art Unit	Examiner
2137	GERGISO, Techane

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 38,342
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

[signature]
Signature

Jeffrey G. Toler
Typed or printed name

512-327-5515
Telephone number

10-19-2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [x] *Total of 1 forms are submitted.

RECEIVED
CENTRAL FAX CENTER
OCT 19 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	James M. Doherty, et al.		
Title:	INTRUSION DETECTION		
App. No.:	10/605,689	Filed:	October 17, 2003
Examiner:	GERGISO, Techane	Group Art Unit:	2137
Customer No.:	60533	Confirmation No.:	2688
Atty. Dkt. No.:	1033-T00534C		

MS: AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REMARKS IN SUPPORT OF THE PRE-APPEAL BRIEF REQUEST FOR REVIEW

Dear Sir:

In response to the Final Office Action mailed July 23, 2007, (hereinafter, "Final Office Action") and further pursuant to the Notice of Appeal and Pre-Appeal Brief Request for Review submitted herewith, Applicants respectfully request review and reconsideration of the Final Office Action in view of the following issues.

1. The Asserted Reference of Moran is Missing an Element of Each of the Claims

Applicants traverse the rejection of claims 1, 10, and 15 under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,647,400 ("Moran"), at page 4 of the Final Office Action. Moran does not disclose upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host, as recited in claim 1. Rather, Moran discloses that if there is a mismatch of signatures, and if the mismatch is not expected, the file associated with the signature is flagged as suspicious. *See* Moran, col. 32, lines 56-58. Moran also discloses a sensor controller 310 that may pass information to an event database and a system that collects data related to logins with multiple sensors, *See* Moran, col. 8, lines 13-16 and col. 23, lines 35-46. Moran does not explicitly disclose issuing an instruction to record an entry in a remote database when a signature mismatch is discovered. Therefore, Moran does not disclose each and every element of claim 1. Hence, claim 1 is allowable.

CERTIFICATE OF TRANSMISSION/MAILING
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents on 10-19-07.

Jeaneaux Jordan
Typed or Printed Name

Signature

Moran does not disclose or suggest a log database that is remote from the host and recording entries corresponding to mismatches between a digital signature stored in the host and a corresponding digital signature in the digital signature database, as recited in claim 10. Instead, Moran discloses that if a mismatch of signatures is discovered and if the mismatch is not expected, the file is flagged as suspicious. *See* Moran, col. 32, lines 56-58. Moran also discloses a sensor controller 310 that may pass information to an event database and a system that collects data related to logins with multiple sensors. *See* Moran, col. 8, lines 13-16 and col. 23, lines 35-46. However, Moran does not explicitly disclose a log database that is remote from the host and recording entries corresponding to digital signature mismatches. Therefore, Moran does not disclose each and every element of claim 10. Hence, claim 10 is allowable.

Moran does not disclose computer readable program code including executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signatures, said entry identifying a possible intrusion in a host, as recited in claim 15. Instead, Moran discloses that if a mismatch of signatures is discovered and if the mismatch is not expected, the file is flagged as suspicious. *See* Moran, col. 32, lines 56-58. Moran does not explicitly disclose issuing an instruction to record an entry in a log file located in a remote database upon identifying a digital signature mismatch. Therefore, Moran does not disclose or suggest each and every element of claim 15. Hence, claim 15 is allowable.

2. The Asserted Combination of Moran and Trostle is Missing an Element of Each of the Claims

Applicants traverse the rejection of claims 2-9, 11-14, and 16-24, at paragraphs 6 and 7 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Moran in view of by U.S. Patent No. 5,919,257 ("Trostle").

As explained previously, Moran does not disclose all elements of claim 1, from which claims 2-9 depend. Trostle does not disclose or suggest the elements of claim 1 not disclosed by Moran. For example, Trostle does not disclose upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host, as recited in claim 1. In contrast, Trostle discloses a login process in which if an invalid password has been entered, a server increments an intruder detection counter, and if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, Fig. 5, col. 5, lines 49-65, and col. 6, lines 29-30, col. 6, lines 30-40. Trostle also discloses that during pre-boot, the networked workstation performs an intrusion detection hashing function on selected executable programs in order to detect unauthorized

changes to the selected workstation executable programs and if illicit changes are detected, the user or network system administrator is notified in order to take corrective action. *See* Trostle, Abstract and col. 2, line 61 – col. 3, line 2. Trostle does not disclose issuing an instruction to record an entry in a log file located in a remote database, the entry identifying a possible intrusion in a host. Therefore, Moran and Trostle, separately or in combination, fail to disclose each and every element of claim 1, or of claims 2-9, which depend from claim 1. Therefore, claims 2-9 are allowable, at least by virtue of their dependence from claim 1.

Further, the dependent claims recite additional features that are not disclosed by the cited references. For example, Moran does not disclose issuing a command to an operating system of the host to bring the host to a single user state upon identifying a mismatch in compared digital signatures, as recited in claim 3. Further, Trostle does not disclose this element. Instead, Trostle discloses that if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, col. 6, lines 30-40, and Fig. 5. Thus, in contrast to claim 3, Trostle disables the NIC, shutting down a connection to the network server, or disables the workstation. For this additional reason, claim 3 is allowable.

As explained above, Moran does not disclose or suggest each and every element of claim 10, from which claims 11-14 depend. Trostle does not disclose or suggest the elements of claim 10 that are not disclosed by Moran. For example, Trostle does not disclose a log database remote from the host recording entries corresponding to mismatches between a digital signature stored in the host and a corresponding digital signature in the digital signature database, as recited in claim 10. In contrast to claim 10, Trostle discloses a login process in which a user enters a user name and a password for validation, and if an invalid password has been entered, a server increments an intruder detection counter. *See* Trostle, col. 5, lines 49-65, col. 6, lines 29-30, and Fig. 5. Applicants submit that a password is not equivalent to a digital signature. In further contrast to claim 10, Trostle discloses that if illicit changes in selected workstation executable programs are detected through comparison of computed hash values of executable programs with trusted hash values downloaded from a server, a user or network system administrator is notified to take corrective action. *See* Trostle, Abstract, and col. 2, line 61 – col. 3, line 2. Trostle does not disclose a log database remote from the host, the log database to record entries corresponding to digital signature mismatches. Therefore, Moran and Trostle, separately or in combination, fail to disclose each and every element of claim 10, or of claims 11-14, which depend from claim 10. Hence claims 11-14 are allowable over the asserted combination.

As explained above, Moran does not disclose each and every element of claim 15, from which claim 16 and 17 depend. Trostle does not disclose or suggest the elements of claim 15 that are not disclosed by Moran. For example, Trostle does not disclose computer readable program code including executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signatures, said entry identifying a possible intrusion in a host, as recited in claim 15. Instead, Trostle discloses that if an invalid password has been entered, a server increments an intruder detection counter. *See* Trostle, Fig. 5, and col. 6, lines 29-30. In further contrast to claim 15, Trostle discloses that the networked workstation performs an intrusion detection hashing function on selected executable programs, and if illicit changes are detected, the user or network system administrator is notified in order to take corrective action. *See* Trostle, Abstract, and col. 2, line 61 – col. 3, line 2. Trostle does not disclose issuing an instruction to record an entry in a log file located in a remote database, the entry identifying a possible intrusion in a host. Thus Moran and Trostle, separately or in combination, fail to disclose or suggest each and every element of claim 15, or of claims 16 and 17, at least by virtue of their dependence from allowable claim 15. Hence, claims 16 and 17 are allowable.

Further, the Office admits that Moran does not disclose computer readable program code comprising executable instructions to issue a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures, as recited in claim 17. *See* Office Action dated Feb. 22, 2007, page 10. In contrast to claim 17, Trostle discloses locking a user out when a maximum number of allowable unsuccessful logins has been exceeded by disabling the NIC. *See* Trostle, Fig. 5, step 100, and col. 6, lines 30-42. Thus, in contrast to claim 17, Trostle disables the NIC, shutting down a connection to the network server. For this additional reason, claim 17 is allowable.

None of the cited references, including Moran and Trostle, separately or in combination, discloses each and every element of claim 18. For example, Moran does not disclose upon identifying a mismatch of digital signatures, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host, as recited in claim 18. In contrast to claim 18, Moran discloses that if there is a mismatch of signatures, an analysis engine checks if the mismatch is expected and if not, the file is flagged as suspicious. *See* Moran, col. 32, lines 56-58. Moran also discloses a sensor controller 310 that may pass information to an event database and a system that collects data related to logins with multiple sensors. *See* Moran, col. 8, lines 13-16 and col. 23, lines 35-46. However, Moran does not explicitly disclose upon identifying a mismatch of digital signatures, transmitting an instruction to a

RECEIVED
CENTRAL FAX CENTER
OCT 19 2007

remote log database via one or more network interfaces, the instruction executed in the remote log database to record an entry in a log file. Further, Trostle does not disclose this element of claim 18. Instead, Trostle discloses that if an invalid password has been entered, a server increments an intruder detection counter. *See* Trostle, Fig. 5, and col. 6, lines 29-30. In further contrast to claim 18, Trostle discloses comparing a computed hash value of an executable program to a trusted hash value to detect illicit changes in the executable program, and notifying the user or system administrator if changes are detected. *See* Trostle, col. 2, line 45 – col. 3, line 2. Trostle does not disclose issuing an instruction to record an entry in a log file located in a remote database, the entry identifying a possible intrusion in a host. Hence, claim 18 is allowable over Moran and Trostle, and claims 19-24, which depend from claim 18, are also allowable.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the references applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the rejections, as well as an indication of the allowability of each of the pending claims

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

10-19-2007
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
TOLER SCHAFFER LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)